

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full “License and Conditions of Use” notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

Annex A. Comparative Positioning of the Deterministic Quantum Hash Framework Relative to Current Models and Integration Pathways

Purpose

This annex situates the deterministic quantum hash framework within the current landscape of quantum hashing, quantum fingerprinting, provenance identification, and reproducible scientific workflow models, and clarifies whether the framework should be interpreted as an integrative extension of existing families or as a novel model class for implementation across multi-scale physical and informational systems.[file:202][web:221][web:232]

A.1 Current Model Landscape

The current landscape is not dominated by a single directly equivalent model.[file:202] Instead, it is composed of partially overlapping families that address different aspects of the problem: quantum fingerprinting and quantum cryptographic hashing, classical provenance and workflow hashing systems, simulation provenance chains, and domain-specific identity schemes for physical or computational artifacts.[web:221][web:225][web:226][web:232]

A.1.1 Quantum Fingerprinting and Quantum Hashing

Quantum fingerprinting and quantum hashing typically map a classical input string into a quantum state that supports tasks such as equality testing, authentication, or communication complexity reduction.[web:221][web:225][web:230][web:234] In these models, the input is generally already a symbolic or binary object, and the principal emphasis is on one-way properties, state distinguishability, or cryptographic communication efficiency rather than on direct construction from multi-scale physical observables.[web:221][web:225][web:230]

A.1.2 Provenance Hashing and Workflow Identity Systems

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full “License and Conditions of Use” notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

A second family includes provenance chains, cascading signatures, digital identifiers, and workflow-based traceability systems used in scientific data processing and simulation management.[web:226][web:229][web:232][web:235] These systems are highly valuable for reproducibility and artifact linkage, but they usually operate on files, scripts, workflow records, or dataset manifests rather than on a formal hybrid descriptor combining state structure, entropy, energy scale, time, and causal constraints.[web:226][web:229][web:235]

A.1.3 Device and Physics-Linked Fingerprinting Systems

A third emerging family includes quantum-device authentication and physical-signature methods that derive a fingerprint from experimentally observed behavior, statistical signatures, or hardware-specific patterns.[web:223] These approaches move closer to physical provenance than classical workflow identifiers, but they tend to be specialized to device attestation or hardware authenticity rather than to a general-purpose descriptor spanning macroscopic physical, computational, and biological domains.[web:223]

A.2 Position of the Present Framework

The deterministic quantum hash framework occupies a distinct position because it does not begin from a raw bit string alone and does not restrict itself to a quantum communication primitive.[file:202] Instead, it defines a structured deterministic mapping from state representation, effective observable summary, entropy, energy scale, temporal indexing, causal consistency, and metadata into a continuous descriptor and then into a cryptographic identifier.[file:202]

This means the framework is neither a direct reformulation of standard quantum fingerprinting nor merely a conventional provenance hash.[file:202][web:221][web:226] It is better understood as a **hybrid physical-informational provenance model** that integrates ideas from quantum statistical representation, entropy-based characterization, deterministic indexing, and modern cryptographic hashing into a single reproducible architecture.[file:202][web:221][web:232]

A.3 Comparative Table

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.

No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.

See full “License and Conditions of Use” notice for details.

In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.

Author: Carlos Daniel Borrego Romero

Model family	Typical input	Typical output	Main strength	Main limitation relative to this framework	Relationship to the present framework
Quantum fingerprinting [web:221][web:222][web:234]	Classical string or symbolic word	Compact quantum state for equality testing or communication tasks	Strong theoretical efficiency in communication and distinguishability tasks [web:221][web:222]	Usually not anchored to physical observables, entropy scaling, or provenance metadata across domains [web:221][file:202]	Provides conceptual inspiration but not a direct operational equivalent
Quantum cryptographic hashing [web:225][web:230][web:233]	Classical input mapped to quantum state	One-way or collision-resistant quantum hash object	Cryptographic and authentication relevance [web:225][web:230]	Focuses on state-level cryptographic construction rather than multi-scale physical-informational indexing [web:225][file:202]	Adjacent family, but narrower in domain scope
Provenance hash chains and workflow identifiers [web:226][web:229][web:232][web:235]	Files, workflows, runtime logs, artifacts	Reproducibility identifiers and provenance chains	Strong traceability of computational artifacts [web:226][web:235]	Usually lacks explicit physical-state, entropy, and operator-based semantics [web:229][file:202]	Highly compatible integration target

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
 No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
 See full “License and Conditions of Use” notice for details.
 In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
 Author: Carlos Daniel Borrego Romero

Quantum-device authentication / physical fingerprinting [web:223]	Device statistics, experimental signatures, metadata	Device-specific fingerprint or attestation record	Physical authenticity and hardware provenance [web:223]	Typically specialized to device verification, not general multi-scale system identification [web:223]	Compatible in the provenance layer, but more specialized
Deterministic quantum hash framework [file:202]	State representation, operator expectation, entropy, energy scale, time, causal descriptor, metadata	Continuous descriptor plus cryptographic deterministic identifier	Multi-scale applicability, physical interpretability, provenance integration, deterministic reproducibility [file:202]	Requires explicit standardization of operator definitions, entropy references, causal coding, and serialization [file:202]	Novel integrative framework

A.4 Why the Framework Is Novel

The present framework is novel in the sense that no directly equivalent model appears in the current literature landscape combining all of the following in a single deterministic scheme: a state-based representation, an effective observable expectation, entropy normalization, macroscopic energy scaling, time-indexed state labeling, causal constraints, and canonical metadata serialization prior to cryptographic hashing.[file:202][web:221][web:226][web:232] Existing quantum hashing literature provides the conceptual background for mapping information into protected or compact signatures, but it does not ordinarily embed the full multi-scale physical-informational construction proposed here.[web:221][web:225][web:230]

The model is therefore best viewed not as a direct competitor to a mature established category, but as a novel implementation candidate that bridges gaps between quantum-information-inspired hashing, scientific provenance, and physically interpretable system identification.[file:202][web:226][web:235]

A.5 Benefits of Integration with Existing Models

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full “License and Conditions of Use” notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

A.5.1 Integration with Quantum Fingerprinting and Quantum Hashing

The framework can benefit from the conceptual and cryptographic insights of quantum fingerprinting and quantum hashing, especially in relation to compact encoding, distinguishability, and hash-theoretic security properties.[web:221][web:225][web:230] In return, it adds a missing layer of physical and provenance semantics by constructing the input from structured system descriptors rather than from arbitrary classical strings alone.[file:202]

A.5.2 Integration with Provenance Systems

The strongest near-term integration pathway is with scientific provenance and workflow systems.[web:226][web:229][web:232][web:235] Provenance chains already capture input files, code versions, execution logs, and data transformations, and the deterministic quantum hash framework can extend this by adding a formal physical-informational descriptor of the system state itself.[file:202][web:235] This would strengthen reproducibility by linking not only artifacts and workflows, but also the interpreted system configuration represented by the model.[file:202]

A.5.3 Integration with Device Authentication and Physical Signatures

In contexts where physical devices or experiments produce distinctive statistical signatures, the framework can serve as a higher-level deterministic descriptor that absorbs these signatures alongside entropy, temporal, and metadata terms.[web:223] This would allow hardware- or experiment-level fingerprints to be embedded into a broader provenance model rather than remaining isolated as specialized attestation objects.[web:223][file:202]

A.6 If No Fully Equivalent Model Exists

Because the literature does not appear to provide a fully equivalent framework with the same physical-informational composition, the present model should be highlighted as a novel framework to be implemented and tested rather than as a minor variant of an established standard.[file:202][web:221][web:226] Its novelty lies in the integration itself: the combination of physically meaningful observables, entropy structure, deterministic temporal and causal labeling, and cryptographic serialization into a reproducible descriptor spanning physical, informational, and biological domains.[file:202]

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full “License and Conditions of Use” notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

This does not imply that all subcomponents are individually new.[file:202] Instead, the originality resides in the way existing conceptual families are fused into a unified architecture with explicit multi-scale applicability and provenance-oriented interpretation.[file:202][web:232][web:235]

A.7 Strategic Value of the Framework

The strategic value of the model is highest in contexts where traditional cryptographic identifiers are too syntactic and traditional scientific provenance models are too artifact-centered.[web:226][web:235] The framework adds a semantically richer identity layer that can encode state structure, scale, disorder, temporal position, and contextual reproducibility within the same deterministic pipeline.[file:202]

This makes it potentially useful for large-scale simulations, reference system indexing, multi-version scientific datasets, biological experimental pipelines, and hybrid AI-assisted provenance systems where one wants to preserve not only file identity but also system-state identity.[file:202][web:229][web:235]

A.8 Conclusions

The deterministic quantum hash framework does not have a direct one-to-one equivalent among current mainstream models.[file:202] It is related to quantum fingerprinting, quantum cryptographic hashing, provenance chain systems, and physical-signature approaches, but it extends beyond each of these by combining physically meaningful observables, entropy normalization, energy scaling, deterministic time and causal structure, and metadata into a single reproducible descriptor.[web:221][web:225][web:226][web:232]

Where existing models are available, the framework is best positioned as an integrative enhancement rather than a replacement.[file:202] Where no equivalent model exists, it should be presented as a novel architecture ready for formal implementation and empirical testing.[file:202] Its most important contribution is the creation of a bridge between physical interpretability and provenance-grade deterministic identification across multiple scientific and informational domains.[file:202][web:235]

LICENSE AND CONDITIONS OF USE.

The content is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license:

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.

No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.

See full "License and Conditions of Use" notice for details.

In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.

Author: Carlos Daniel Borrego Romero

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

By using this content and model, you agree to:

Provide appropriate credit, include a link to the above license, and indicate if changes were made.

Not use the material or any derivative works for commercial purposes.

Distribute any adaptations or derivative works only under the same CC BY-NC-SA 4.0 license.

Not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Data logging and trade secrets policy.

The design, implementation, and deployment of this model, as well as any derivatives, do not authorize the collection, storage, or exploitation of IP addresses, unique device identifiers, or other technical traceability data for commercial profiling, targeted advertising, or any other economic exploitation.

Any system implementing this model must limit the logging and retention of IP addresses and other identifiable data strictly to what is necessary to:

(a) maintain technical security and service integrity; and

(b) comply with applicable legal obligations (for example, any minimum log retention required by law).

It is prohibited to use this model or its derivatives to:

capture, store, or exploit trade secrets, proprietary know-how, or confidential information of users or third parties for any purpose other than providing the technical service described in this documentation; or train or improve closed, commercial systems using data that contains confidential information of third parties without their prior, explicit, written consent.

---+EOD+---